Analyse der Zähler für Krypto-ACLs in richtlinienbasierten VPN-Tunneln

Inhalt

Einleitung

Voraussetzungen

- Anforderungen
- Verwendete Komponenten

Topologie

Szenarien

- Szenario 1: Datenverkehr, der von Router1 initiiert wird, während der VPN-Tunnel inaktiv ist
- Szenario 2: Datenverkehr, der von Router2 initiiert wird, während der VPN-Tunnel aktiv ist

Konfiguration

- Verschlüsselungskonfiguration auf Router1
- Verschlüsselungskonfiguration auf Router 2

Verhaltensanalyse der Zähler der Krypto-Zugriffskontrollliste in VPN-Tunneln

- Szenario 1: Datenverkehr, der von Router1 initiiert wird, während der VPN-Tunnel inaktiv ist
- Zweites Szenario: Datenverkehr, der von Router 2 initiiert wird, während der VPN-Tunnel aktiv ist

Fazit:

Wichtigste Punkte:

Einleitung

In diesem Dokument wird das Verhalten der ACL-Zähler (Crypto Access Control List) in richtlinienbasierten VPN-Tunneln beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, sich mit folgenden Themen vertraut zu machen:

- Richtlinienbasiertes Site-to-Site-VPN auf Cisco IOS®/Cisco IOS® XE-Plattform
- Zugriffskontrolllisten auf der Cisco IOS/Cisco IOS XE-Plattform

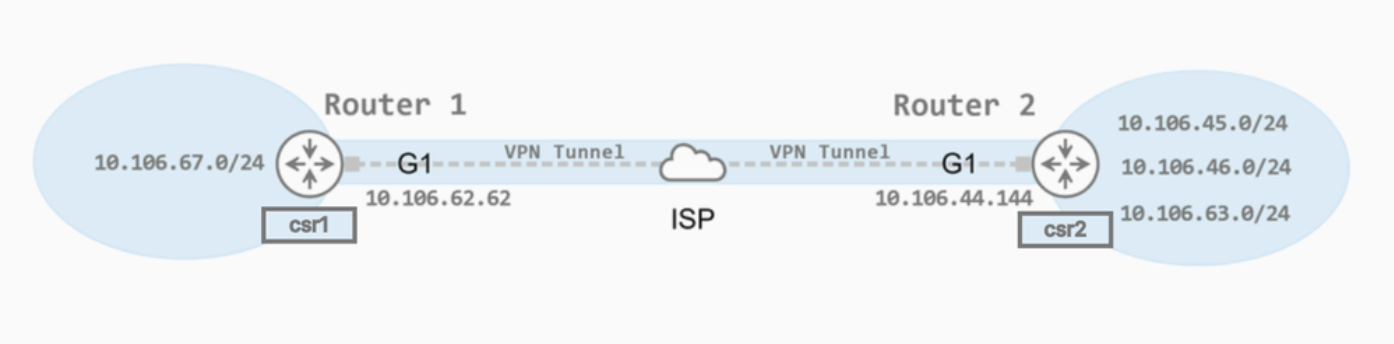
Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco C8kv, Version 17.12.04 (MD)

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Topologie



Topologie

Szenarien

Durch die Untersuchung zweier unterschiedlicher Szenarien soll ermittelt werden, wie sich die Zugriffskontrolllistenanzahl auf den Datenverkehr auswirkt, der von verschiedenen Peers initiiert wird, und wie sich die Tunnel zurücksetzen.

1. Szenario 1: Datenverkehr, der von Router1 initiiert wird, während der VPN-Tunnel inaktiv ist

   In diesem Szenario werden die Änderungen bei der Anzahl der ACL-Treffer analysiert, wenn der VPN-Tunnel zu Beginn ausfällt und der Datenverkehr von Router1 initiiert wird. Diese Analyse hilft, die anfängliche Einrichtung zu verstehen und wie die Krypto-ACL-Zähler auf den ersten Datenverkehrsflusstest reagieren.

2. Szenario 2: Datenverkehr, der von Router2 initiiert wird, während der VPN-Tunnel aktiv ist

   In diesem Szenario ist der VPN-Tunnel bereits eingerichtet, und der Datenverkehr, der vom Router 2 initiiert wird, wird untersucht. Dieses Szenario bietet Einblicke in das Verhalten von ACL-Zählern, wenn der Tunnel aktiv ist und Datenverkehr von einem anderen Peer stammt.

Durch den Vergleich dieser Szenarien können wir ein umfassendes Verständnis der Dynamik von ACL-Zählern in VPN-Tunneln unter unterschiedlichen Bedingungen gewinnen.

Konfiguration

Wir haben einen richtlinienbasierten Site-to-Site-VPN-Tunnel zwischen zwei als Peers designierten Cisco C8kv-Routern konfiguriert. Router1 heißt "csr1" und Router2 "csr2".

Verschlüsselungskonfiguration auf Router1

```
csr1#sh ip int br
Interface              IP-Address      OK?   Method   Status  Protocol
GigabitEthernet1       10.106.62.62    YES   NVRAM    up      up
GigabitEthernet2       10.106.67.27    YES   NVRAM    up      up
```

```
csr1#sh run | sec crypto map
crypto map nigarapa_map 100 ipsec-isakmp
   set peer 10.106.44.144
   set transform-set new_ts
   set ikev2-profile new_profile
   match address new_acl
```

```
csr1#sh ip access-lists new_acl
Extended IP access list new_acl
   10 permit ip 10.106.67.0 0.0.0.255 10.106.45.0 0.0.0.255 log
   20 permit ip 10.106.67.0 0.0.0.255 10.106.46.0 0.0.0.255
   30 permit ip 10.106.67.0 0.0.0.255 10.106.63.0 0.0.0.255 log
```

```
csr1#sh run int GigabitEthernet1
Building configuration...

Current configuration : 162 bytes
!
interface GigabitEthernet1
ip address 10.106.62.62 255.255.255.0
ip nat outside
negotiation auto
no mop enabled
no mop sysid
crypto map nigarapa_map
end
```

Verschlüsselungskonfiguration auf Router 2

```
csr2#sh ip int br
Interface              IP-Address        OK?     Method       Status     Protocol
GigabitEthernet1       10.106.44.144     YES     NVRAM        up         up
GigabitEthernet2       10.106.45.145     YES     NVRAM        up         up
GigabitEthernet3       10.106.46.146     YES     NVRAM        up         up
```

```
GigabitEthernet4       10.106.63.13       YES      NVRAM         up          up
```

```
csr2#sh run | sec crypto map
crypto map nigarapa_map 100 ipsec-isakmp
   set peer 10.106.62.62
   set transform-set new_ts
   set ikev2-profile new_profile
   match address new_acl
```

```
csr2#sh ip access-lists new_acl
Extended IP access list new_acl
   10 permit ip 10.106.45.0 0.0.0.255 10.106.67.0 0.0.0.255
   20 permit ip 10.106.46.0 0.0.0.255 10.106.67.0 0.0.0.255
   30 permit ip 10.106.63.0 0.0.0.255 10.106.67.0 0.0.0.255
```

```
csr2#sh run int GigabitEthernet1
Building configuration...

Current configuration : 163 bytes
!
interface GigabitEthernet1
ip address 10.106.44.144 255.255.255.0
ip nat outside
negotiation auto
no mop enabled
no mop sysid
crypto map nigarapa_map
end
```

Verhaltensanalyse der Zähler der Krypto-Zugriffskontrollliste in VPN-Tunneln

Zunächst haben beide Geräte in ihren jeweiligen Krypto-Zugriffslisten einen ACL-Trefferzähler von Null.

Die Anzahl der Treffer in der Zugriffskontrollliste für die jeweiligen Krypto-Zugriffslisten auf den beiden Peer-Geräten betrug null.

Szenario 1: Datenverkehr, der von Router1 initiiert wird, während der VPN-Tunnel inaktiv ist

Anfangszustand:

Der VPN-Tunnel, der Router1 (IP: 10.106.67.27) und Router2 (IP: 10.106.45.145) ist derzeit inaktiv.

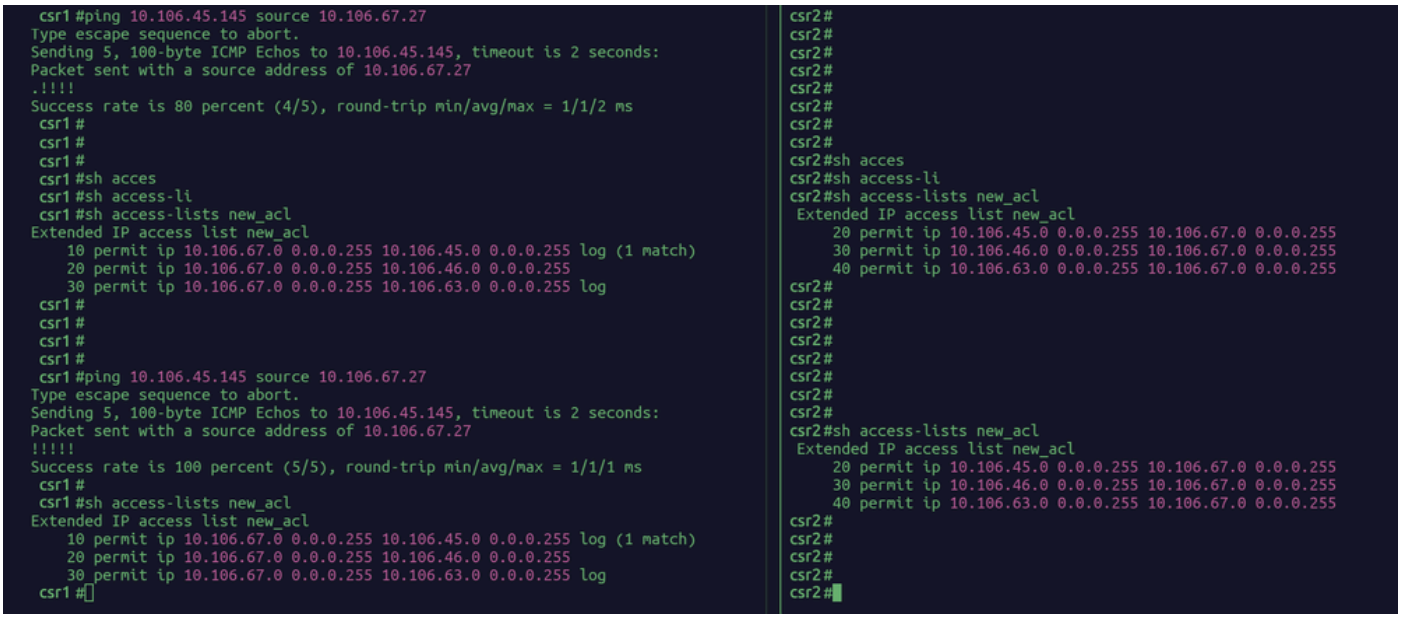
Durchgeführte Aktion:

Datenverkehr wird von Router1 initiiert, der die Kommunikation mit Router2 herstellen soll.

Anmerkungen:

1. ACL-Indikatorverhalten:
   antwort: Beim Initiieren des Datenverkehrs von Router1 erfolgt auf Router1 ein merklicher Anstieg des ACL-Zählers (Access Control List, Zugriffskontrollliste). Dieser Anstieg tritt nur ein Mal auf, wenn der Tunnel versucht, den Datenverkehr einzurichten.
   b. Der Anstieg des ACL-Zählers wird ausschließlich auf dem initiierenden Router, in diesem Szenario Router1, beobachtet. Router2 zeigt zu diesem Zeitpunkt keine Änderungen am ACL-Zähler an.
2. Tunnelaufbau:
   antwort: Nach der ersten Erhöhung, die der Initiierung des Datenverkehrs entspricht, wird der Tunnel zwischen dem ersten und dem Router2 erfolgreich eingerichtet.
   b. Nach der Einrichtung des Tunnels stabilisiert sich der ACL-Zähler auf Router1 und zeigt keine weiteren Inkremente an. Dies zeigt an, dass die ACL-Regel erfüllt wurde und nun konsistent Datenverkehr durch den eingerichteten Tunnel fließt.
3. Tunnel-Neuinitiierung:
   Der ACL-Zähler auf Router1 wird nur dann um einen weiteren Wert erhöht, wenn der Tunnel ausfällt und wiederhergestellt werden muss. Dies deutet darauf hin, dass die ACL-Regel durch die Initiierung des Datenverkehrs ausgelöst wird, der den Tunnel einzurichten versucht, und nicht durch die fortlaufende Datenübertragung, sobald der Tunnel aktiv ist.

Zusammenfassend zeigt dieses Szenario, dass der ACL-Zähler auf Router1 empfindlich für die anfänglichen Datenverkehrsversuche zur Tunnelerstellung ist, aber statisch bleibt, sobald der VPN-Tunnel betriebsbereit ist.



Zweites Szenario: Datenverkehr, der von Router 2 initiiert wird, während der VPN-Tunnel aktiv ist

Anfangszustand:

Der VPN-Tunnel, der Router1 (IP: 10.106.67.27) und Router2 (IP: 10.106.45.145) ist derzeit aktiv und in Betrieb.

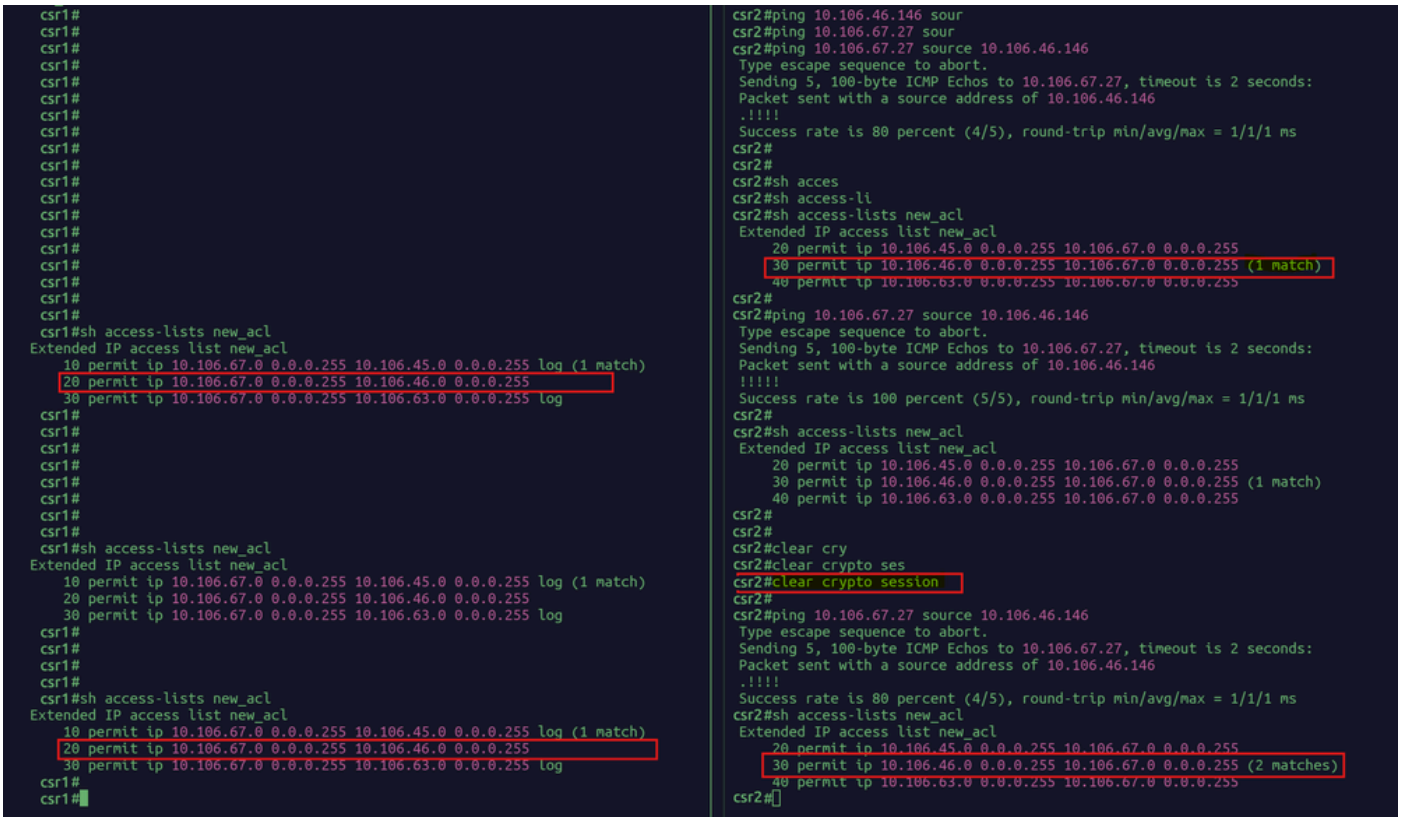
Durchgeführte Aktion:

1. Der Datenverkehr wird von Router2 in Richtung Router1 initiiert, während der Tunnel betriebsbereit ist.
2. Anschließend wird der Tunnel gezielt geräumt (oder zurückgesetzt).
3. Nachdem der Tunnel geräumt wurde, leitet Router2 erneut Datenverkehr ein, um die Verbindung wiederherzustellen.

Anmerkungen:

1. Anfängliche Datenverkehrsinitiierung:
   antwort: Wenn der Datenverkehr zum ersten Mal von Router2 initiiert wird, während der Tunnel bereits eingerichtet ist, findet keine sofortige Änderung im ACL-Zähler (Access Control List) statt.
   b. Dies weist darauf hin, dass der fortlaufende Datenverkehr innerhalb eines bereits eingerichteten Tunnels keinen Inkrement des ACL-Zählers auslöst.
2. Tunnellöschung und -neuinitiierung:
   antwort: Beim Löschen des Tunnels wird die bestehende Verbindung zwischen dem ersten Router und Router2 vorübergehend unterbrochen. Dies erfordert einen Wiederherstellungsprozess für jeden nachfolgenden Datenverkehr.
   b. Wenn der Datenverkehr von Router2 erneut initiiert wird, nachdem der Tunnel gelöscht wurde, erfolgt ein sichtbarer Anstieg des ACL-Zählers auf Router2. Dieser Anstieg bedeutet, dass die ACL-Regeln erneut aktiviert werden, um die Erstellung des Tunnels zu erleichtern.
3. Spezifität des ACL-Zählers:
   Das Inkrement des ACL-Zählers erfolgt ausschließlich auf der Seite, die den Datenverkehr initiiert, in diesem Fall Router2. Dieses Verhalten unterstreicht die Rolle der ACL bei der Überwachung und Steuerung von Prozessen zur Initiierung von Datenverkehr auf der Ursprungsseite, während der ACL-Zähler von Router1 in dieser Phase unbeeinflusst bleibt.

Zusammenfassend zeigt dieses Szenario, dass der ACL-Zähler auf Router2 beim Wiederherstellen eines VPN-Tunnels auf die Initiierung von Datenverkehr reagiert. Der Zähler erhöht sich nicht mit dem regulären Datenverkehrsfluss innerhalb eines aktiven Tunnels, sondern reagiert auf die erforderliche Wiederherstellung des Tunnels, um eine präzise Verfolgung der Tunnelinitiierungsereignisse sicherzustellen.



Szenario 2

Fazit:

Das Verhalten der Krypto-ACL-Zähler zeigt, dass sie Trefferzählungen ausschließlich während der Initiierungsphase des VPN-Tunnels registrieren.

Initiatorspezifisches Inkrement: Wenn der Tunnel von Router1 initiiert wird, wird die Zunahme der Trefferanzahl nur auf Router1 beobachtet. Wenn die Initiierung von Router2 erfolgt, steigt die Trefferanzahl nur auf Router2 an. Dies unterstreicht die Rolle der ACL bei der Überwachung des Datenverkehrsinitiierungsprozesses an der Quelle.

Stabilität nach Einführung: Sobald der Tunnel erfolgreich eingerichtet wurde, bleiben die ACL-Zähler auf beiden Peers unverändert und zeigen keine weiteren Treffer an. Diese Stabilität bleibt erhalten, bis der Tunnel entweder gelöscht oder zurückgesetzt wird und der Datenverkehr erneut initiiert werden soll.
Dieses Verhalten unterstreicht die Funktionalität von Access Control Lists bei der Nachverfolgung und Steuerung der Anfangsphase der Tunnelerstellung. So wird sichergestellt, dass der nachfolgende Datenfluss innerhalb des erstellten Tunnels die Trefferanzahl nicht beeinflusst.

Wichtigste Punkte:

ACL-Indikatorverhalten: Die ACL-Zähler registrieren während des Tunnelinitiierungsprozesses Inkremente ausschließlich auf der Initiatorseite. Dies zeigt an, dass die Zähler so konzipiert sind, dass sie den anfänglichen Datenverkehr überwachen, der den Tunnelaufbau auslöst.

Statische Zähler nach der Einrichtung: Sobald der Tunnel aktiv und eingerichtet ist, bleiben die

ACL-Zähler unverändert. Sie spiegeln keine weiteren Aktivitäten wider, es sei denn, der Tunnel wird zurückgesetzt und muss neu initiiert werden, was den Fokus auf die anfänglichen Datenverkehrsereignisse unterstreicht.

Spezifität der Datenverkehrsinitiierung: Die Anzahl der ACL-Treffer richtet sich nach dem Peer, der den Tunnel initiiert. Diese Spezifität gewährleistet eine genaue Nachverfolgung, welche Seite für die Initiierung der VPN-Verbindung verantwortlich ist, und ermöglicht eine genaue Überwachung und Steuerung.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.